Chapter 18 - Security Classification

1801 Classification Principles

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life. However, our nation's democratic principles also require that the American people be informed of the activities of their Government; therefore, information may not be classified unless its disclosure reasonably could be expected to cause damage to the national security. Accordingly, security classification shall be applied only to protect the national security. With the exception of the Atomic Energy Act of 1954, as amended, and the National Security Act of 1947, as amended, Executive Order (E.O.) 12958, Classified National Security Information, as amended by Executive Order 13292, provides the only basis for classifying national security information.

1802 Classification Levels

A. National security information that requires protection against unauthorized disclosure shall be classified by an authorized original classification authority (OCA) at one of the following three levels.

1. **Top Secret** shall be applied to information that reasonably could be expected to cause exceptionally grave damage to the national security if disclosed to unauthorized sources.

2. **Secret** shall be applied to information that reasonably could be expected to cause serious damage to the national security if disclosed to unauthorized sources.

3. **Confidential** shall be applied to information that reasonably could be expected to cause damage to the national security if disclosed to unauthorized sources.

B. Except as provided by statute, no additional terms such as "Sensitive," "Conference," "Agency," "Business," or "Administratively" shall be used in conjunction with any of the three classification levels defined above.

1803 Original Classification Standards

A. Information may be originally classified under the terms of E.O. 12958 only if all of the following conditions are met.

1. An OCA classifies the information;

2. The information is owned by, produced by or for, or is under the control of the U.S. Government;

3. The information falls within one or more of the categories of information listed in paragraph 1804 below; and

4. The OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the OCA is able to identify or describe the damage.

B. At the time of the decision, there is no requirement for the classifying authority to prepare a written description of such damage; however, the classifying authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

C. Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

1804 Classification Authority

A. Based on E.O. 12958, the authority to classify original information at the Secret or Confidential level may be exercised only by the Secretary of Commerce and officials to whom such authority has been delegated in accordance with paragraphs B and C below. No Department of Commerce official is authorized to classify original information at the Top Secret level. Officials authorized to classify information at the Secret level are also authorized to classify information at the Confidential level.

B. The authority to classify original information in the Department may be delegated only to those positions that have a demonstrable and continuing need to exercise such authority. Incumbents occupying these positions must have a security clearance at the appropriate level. Classifying authority delegated by the Secretary cannot be re-delegated but may be exercised by persons designated in writing to act in the absence of the designated classifying authority, provided they have the appropriate level of security clearance. The delegation of original

classifying authority will be limited to the minimum number of individuals absolutely required for efficient administration and protection of Departmental programs.

C. Requests for delegation of authority to perform original classification actions shall be made to the Secretary of Commerce through the Director for Security. The request shall identify the proposed recipient by position, operating unit, and the level of classification authority requested. The request must also include adequate justification for the OCA delegation.

D. Prior to assigning a classification, an OCA shall refer to the Department of Commerce National Security Classification Guide to determine if the information requiring classification is addressed in the classification guide. If not, the OCA may classify the information as an "original classification decision," provided it is not derived from another source. OCAs are encouraged to consult with their security contacts or their servicing security officer for assistance when classifying information. OCAs shall keep records of all original classification decisions and shall provide this information upon request to their servicing security officer. This record is required in order to comply with internal review and evaluation requirements of E.O. 12958 as well as annual reporting requirements of classification decisions.

E. All original and derivative classification and declassification decisions must be reported annually on the SF-311, as described in paragraph 1707. To compile the necessary data, each OCA shall report all original and derivative classification and declassification decisions by maintaining accurate records of all decisions made. Effective record keeping is essential in complying data for this annual report. Each OCA shall work in coordination with the servicing security officer to ensure a reliable tracking and recording system is utilized. In addition, the head of each office that generates derivative classification actions must maintain accurate records of all decisions made. A report of no classification actions must be made also. Input shall be submitted from each operating unit or servicing security officer to the Office of Security in Washington, D.C. The security officer must retain the completed SF-311 with data provided by each OCA and unit head regarding original and derivative classification, and/or declassification decisions made during each fiscal year. All decisions may be challenged, therefore, file records must be maintained.

F. Each OCA shall ensure their operating unit records systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate the declassification of records under the provisions of E.O. 12958 when such information no longer meets the standards for continued classification.

G. On an annual basis, the Director for Security shall review the need for OCA in each operating unit. The Director for Security may recommend withdrawing classifying authority when no demonstrated or continuing need exists for the official to exercise this authority, upon failure of the official to provide adequate justification

for continuing use of the authority, or if an official is in violation of one or more of the E.O. 12958 provisions. If a demonstrated or continuing need for OCA should arise subsequent to a revocation, a new request for delegation shall be submitted.

H. The Office of Security shall provide or ensure OCA training is conducted by the security contacts or servicing security officers as directed by E.O. 12958 and the Implementing Directive for E.O. 12958 (32 CFR Part 2001).

1805 Classification Categories

Information may be classified when it concerns one or more of the categories listed below, and when the unauthorized disclosure of the information, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security. Information may not be classified unless it concerns:

A. Military plans, weapons systems, or operations;

B. Foreign government information;

C. Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

D. Foreign relations or foreign activities of the United States, including confidential sources;

E. Scientific, technological, or economic matters relating to the national security;

F. U.S. Government programs for safeguarding nuclear materials or facilities;

G. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or

H. Weapons of mass destruction.

1806 Duration of Classification under E.O. 12958

A. OCAs shall follow the sequence listed below when determining the duration of classification for information originally classified under E.O. 12958, Classified National Security Information.

1. At the time of original classification, the OCA shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date or event shall not exceed the time frame noted below.

2. If an OCA cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the OCA otherwise determines that the sensitivity of the information requires that it shall be marked for declassification 25 years from the date of the original decision. All information classified according to guidance contained in E.O. 12958, as amended, shall be subject to automatic declassification provisions if it contains records of permanent historical value.

3. An OCA may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under E.O. 12958, as amended, are followed. An OCA may extend the duration of classification for information contained in non-permanent records beyond 25 years in accordance with the standards and procedures for classifying information under E.O. 12958, as amended, except for information that identifies a confidential human source or a human intelligence source. However, the OCA shall identify a specific date or event for declassification of the information when extending the classification beyond 25 years.

4. When extending the duration of classification, the OCA must:

a. Be an OCA with jurisdiction over the information;

b. Ensure that the information continues to meet the standards for classification under the Order; and

c. Make reasonable attempts to notify all known holders of the information.

B. Extensions of classification are not automatic. If an OCA with jurisdiction over the information does not extend the classification of information that has an assigned date or event for declassification, the information is automatically declassified upon the occurrence of the date or event.

C. Information marked for an indefinite duration of classification under predecessor orders such as "Originating Agency's Determination Required" or its acronym "OADR" or information classified under predecessor orders that contain no declassification instructions shall be declassified according to Chapter 19, Declassification and Downgrading.

1. An authorized declassification authority with jurisdiction over the information may declassify the information and release it unless withholding is otherwise authorized and warranted under applicable law.

2. An authorized OCA with jurisdiction over the information may specify a date or event for declassification.

3. Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to automatic declassification procedures of E.O. 12958.

Note: It is recommended that each year during the annual classified material inventory, all classified documents be reviewed and evaluated for further retention, possible declassification or destruction.

1807 Tentative Classification

When an employee, contractor, licensee, certificate holder, or grantee of the Department that does not have the authority to make original classification decisions develops information requiring classification, the individual shall safeguard the information in the manner prescribed according to its intended classification. The developer shall forward the tentatively classified information to an appropriate OCA for a classification decision. OCAs will have 30 days from the date of the classification request to make a classification determination. If it is not clear which OCA has classification responsibility for this information, the holder of the information shall forward the information, with appropriate recommendations, to the Director for Security to determine which OCA has primary subject matter interest. The Office of Security maintains a list of senior executives who have been granted original classification authority. If it cannot be determined which OCA has primary subject matter interest, the Director for Security will make a classification decision on behalf of the Department or forward the information to the Director of the Information Security Oversight Office for a determination.

1808 Department of Commerce National Security Classification Guide

A. A classification guide is written guidance that is issued for a particular program, project, or class of documents to ensure proper and uniform classification of information. The Department of Commerce National Security Classification Guide (Appendix J) has been developed to establish uniform classification levels for frequently recurring items of national security information throughout the Department. The Guide consists of a series of predetermined classification decisions that individuals who are authorized to exercise original classification authority may reference when making classifying decisions. The use of an item in the Guide to classify a document is considered a derivative classification decision.

B. Original classification authority is not required for individuals using the guide. Employees who generate information that requires classification are authorized to classify that information by citing the applicable item in the guide and applying the classification level. Employees also will indicate the date or event for declassification that the guide prescribes. Officials occupying OCA-delegated positions should invoke original classification only when no appropriate item can be identified in the guide.

C. When original classification decision is applied to a category of information not covered, inadequately covered, or improperly covered by this guide, the classifier or responsible component should inform the Office of Security. When it becomes apparent that classification is applied to information not covered or inadequately covered in the guide, then the Office of Security will take action to update the guide. The guide is the standard reference for national security classification actions in Commerce and, therefore, is continuously subject to review and update.

D. An OCA may elect to develop a supplemental classification guide that is specific to their program area. Guides are needed to identify information that truly warrants protection in the interests of national security and to expedite classification decisions. A guide should:

1. Identify the subject matter of the classification guide;

2. Identify the original classification authority by name or identifier and position;

3. Identify an agency point-of-contact for questions regarding the classification guide;

4. Provide the date of issuance or last review;

5. State precisely the elements of information to be protected;

6. State which classification level applies to each element of information, and when useful, specify the elements of information that are unclassified;

7. State, when applicable, special handling requirements;

8. Prescribe declassification instructions or the exemption category from automatic declassification for each element of information. When reviewing or updating a guide, the duration of classification prescribed for each element of information shall be calculated from the date of the information's origin. In addition, when

citing the exemption category listed paragraph 1904, Automatic Declassification, the guide shall also specify the applicable statute, treaty, or international agreement; and,

9. State a concise reason for classification that at a minimum cites the applicable classification category or categories in paragraph 1805.

E. Classification guides should be prepared in all areas where there exists a demonstrated need for a guide. Each classification guide shall be approved in writing by the individual who has program or supervisory responsibility over the information and has been delegated original classification authority at the highest level prescribed in the guide. The classification guide shall be coordinated with the Office of Security.

F. Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. In addition, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide. Classification guides shall be reviewed and updated as circumstances require, but, as a minimum, at least once every five years.

1809 Limitations on Classifying Information

A. Information shall not be classified to:

1.Conceal violations of law, inefficiency, or administrative error;

2. Prevent embarrassment to a person, organization, or agency;

3. Restrain competition;

4. Prevent or delay the release of information that does not require protection in the interest of national security;

5. Classify basic scientific research information not clearly related to the national security; or

B. Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

1. The reclassification action is taken under the personal authority of the Secretary or Deputy Secretary of

Commerce, who determines in writing that the reclassification of the information or documents is necessary in the interest of the national security;

2. The information or documents may be reasonably recovered; and

3. The reclassification action is reported promptly to the Director of the Information Security Oversight Office.

C. Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after the Department has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory declassification review provisions of E.O. 12958, as amended, only if such classification meets the requirements of the Executive Order and is accomplished on a document-by-document basis under the direction of the Director for Security.

D. Compilations or aggregation of pre-existing items of information, which are individually unclassified, may be classified if the compiled information reveals an additional association or relationship that:

1. Meets the standards for classification under E.O. 12958, as amended; and

2. Is not otherwise revealed in the individual items of information.

1810 Classification Challenges

A. E.O. 12958, Classified National Security Information, encourages authorized holders of classified information to challenge classification decisions as a means of promoting proper and thoughtful classification actions. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific classified information in accordance with Section 4.2(g) of E.O. 12958. Authorized holders shall present such challenges to an OCA who has jurisdiction over the information. A formal challenge under this provision shall be in writing and coordinated with the Office of Security. The challenger shall include a statement why he or she believes the information should not be classified or should be classified at a different level.

B. Classification challenges shall follow the procedures outlined below.

1. The Office of Security shall maintain a system for processing, tracking, and recording formal classification challenges made by authorized holders. Records of challenges shall be subject to oversight by the Interagency Security Classification Appeals Panel. Classification challenges shall be considered separately

from Freedom of Information Act or other access requests.

2. The Office of Security shall ensure that each challenge is reviewed by an OCA with jurisdiction over the challenged information. If the challenger is not satisfied with the decision, the challenger may request a review by an impartial official or panel of the originating agency.

3. The OCA reviewing a classification challenge shall provide a written response to a challenger within 60 days. If the OCA is unable to complete his/her review of the classification challenge within 60 days, the OCA must notify the Office of Security and provide a date by which he or she will respond. The Office of Security will inform the challenger and state that if no response from the OCA is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if the Director for Security has not responded to an internal appeal within 90 days of the receipt of the appeal.

C. Denied challenges shall include, at a minimum:

1. A concise reason for denial of the challenge, unless such reason would reveal additional classified information;

2. The names or titles of the officials reviewing the challenge; and

3. The challenger's rights to appeal, including procedures for forwarding the appeal to the Interagency Security Classification Appeals Panel. The Department is not required to process a challenge on information that has been the subject of a challenge within the past two years, or the subject of pending litigation. The Office of Security shall inform the challenger of his or her appeal rights.

D. Challengers and OCAs should attempt to keep all challenges, appeals, and responses unclassified; however, classified information contained in a challenge, a departmental response, or an appeal shall be handled and protected in accordance with E.O. 12958 and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

E. The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be used as a means of minimizing the number of formal challenges.

1811 Derivative Classification

A. Unlike original classification, derivative classification is incorporating, paraphrasing, re-stating, or generating in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification. With the appropriate security clearance, Department of Commerce employees involved in the production or generation of information based on previously classified information are authorized to derivatively classify information.

B. The overall classification markings and portion markings of the source document should supply adequate classification guidance to the derivative classifier. If portion markings or classification guidance are not found in the source document and no reference is made to an applicable classification guide, guidance should be obtained from the originator of the source document. If such markings or guidance are not available, the derivative classifier shall classify the extracted information using the overall classification of the source document.

C. Personnel applying derivative classification to classified material shall follow the guidance noted below.

1. Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Persons who apply derivative classification markings shall:

a. Observe and respect original classification decisions;

b. Carry forward the pertinent classification markings to newly created documents;

c. Apply the date or event for declassification that corresponds to the longest period of classification when the information is based on multiple sources;

d. Attach a listing of classified source(s) to the official file or record copy; and

e. Maintain a copy of the source document, or information identifying the source document with the record or file copy of the newly created document.

2. If the derivative classifier disagrees with the classification of a source document, the classifier may challenge the original classification decision through the Office of Security under the provisions of paragraph

1810 above.

1812 Policy on Transfer of Scientific, Technical, and Engineering Information

National Security Decision Directive 189 provides the national policy for controlling the flow of science, technology, and engineering information produced in federally funded fundamental research at colleges, universities, and laboratories. This directive requires Federal agencies to: 1) determine whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, control the research results through standard classification procedures; and 2) periodically review all research grants, contracts, or cooperative agreements for potential classification.